CLAIMS

What is claimed is:

1. A method for application program obfuscation, comprising:

   receiving a reference to a decryption algorithm and a first cryptographic key;

   creating a key decryption program comprising an instruction stream, said key decryption program configured to perform said decryption algorithm for said first cryptographic key;

   applying a cryptographic process to a second cryptographic key together with said first cryptographic key to create an encrypted second cryptographic key;

   scrambling said encrypted second cryptographic key into said instruction stream using a code obfuscation method indicated by an obfuscation descriptor, said scrambling creating an obfuscated key decryption program, said obfuscation descriptor based at least in part on a target ID; and

   sending said obfuscated key decryption program.

2. The method of claim 1, further comprising sending digital content protected by said second cryptographic key.

3. The method of claim 2, further comprising sending said obfuscated key decryption program together with said digital content.

4. The method of claim 1 wherein said target ID comprises a VM ID.

5. A method for application program obfuscation, comprising:

receiving an obfuscated key decryption program comprising an instruction stream configured to perform a decryption algorithm for a first cryptographic key, said obfuscated decryption program having an encrypted second cryptographic key scrambled in said instruction stream, said second cryptographic key encrypted with said first cryptographic key;

executing said program to decrypt said second cryptographic key; and

decrypting digital content using said second cryptographic key.

6. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for application program obfuscation, the method comprising:

receiving a reference to a decryption algorithm and a first cryptographic key;

creating a key decryption program comprising an instruction stream, said key decryption program configured to perform said decryption algorithm for said first cryptographic key;

applying a cryptographic process to a second cryptographic key together with said first cryptographic key to create an encrypted second cryptographic key;

scrambling said encrypted second cryptographic key into said instruction stream using a code obfuscation method indicated by an obfuscation descriptor, said scrambling creating an obfuscated key decryption program, said obfuscation descriptor based at least in part on a target ID; and

sending said obfuscated key decryption program.

7. The program storage device of claim 6, said method further comprising sending digital content protected by said second cryptographic key.

8. The program storage device of claim 7, said method further comprising sending said obfuscated key decryption program together with said digital content.

9. The program storage device of claim 6 wherein said target ID comprises a VM ID.

10. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for application program obfuscation, the method comprising:

receiving an obfuscated key decryption program comprising an instruction stream configured to perform a decryption algorithm for a first cryptographic key, said obfuscated decryption program having an encrypted second cryptographic key scrambled in said instruction stream, said second cryptographic key encrypted with said first cryptographic key;

executing said program to decrypt said second cryptographic key; and decrypting digital content using said second cryptographic key.

11. An apparatus for application program obfuscation, comprising:

means for receiving a reference to a decryption algorithm and a first cryptographic key;

means for creating a key decryption program comprising an instruction stream, said key decryption program configured to perform said decryption algorithm for said first cryptographic key;

means for applying a cryptographic process to a second cryptographic key together with said first cryptographic key to create an encrypted second cryptographic key;

means for scrambling said encrypted second cryptographic key into said instruction stream using a code obfuscation method indicated by an obfuscation descriptor, said scrambling creating an obfuscated key decryption program, said obfuscation descriptor based at least in part on a target ID; and

means for sending said obfuscated key decryption program.

12. The apparatus of claim 11, further comprising means for sending digital content protected by said second cryptographic key.

13. The apparatus of claim 12, further comprising means for sending said obfuscated key decryption program together with said digital content.

14. The apparatus of claim 11 wherein said target ID comprises a VM ID.

15. An apparatus for application program obfuscation, comprising:

means for receiving an obfuscated key decryption program comprising an instruction stream configured to perform a decryption algorithm for a first cryptographic key, said obfuscated decryption program having an encrypted second cryptographic key scrambled in said instruction stream, said second cryptographic key encrypted with said first cryptographic key;

means for executing said program to decrypt said second cryptographic key; and

means for decrypting digital content using said second cryptographic key.

16. An apparatus for application program obfuscation, comprising an application program provider configured to:

receive a reference to a decryption algorithm and a first cryptographic key;

create a key decryption program comprising an instruction stream, said key decryption program configured to perform said decryption algorithm for said first cryptographic key;

apply a cryptographic process to a second cryptographic key together with said first cryptographic key to create an encrypted second cryptographic key;

scramble said encrypted second cryptographic key into said instruction stream using a code obfuscation method indicated by an obfuscation descriptor, said scrambling creating an obfuscated key decryption program, said obfuscation descriptor based at least in part on a target ID; and send said obfuscated key decryption program.

17. The apparatus of claim 16, said application program provider further configured to send digital content protected by said second cryptographic key.

18. The apparatus of claim 17, said application program provider further configured to send said obfuscated key decryption program together with said digital content.

19. The apparatus of claim 16 wherein said target ID comprises a VM ID.

20. An apparatus for application program obfuscation, comprising a target device configured to:

receive an obfuscated key decryption program comprising an instruction stream configured to perform a decryption algorithm for a first cryptographic key, said obfuscated decryption program having an encrypted second cryptographic key scrambled in said instruction stream, said second cryptographic key encrypted with said first cryptographic key;

execute said program to decrypt said second cryptographic key; and

decrypt digital content using said second cryptographic key.